v1.2020

Contentsquare Supplier Standards

Contentsquare is committed to safeguarding itself and its customers' privacy, security and general compliance. This document represents your required attestation of compliance to Contentsquare and its customers' security, data privacy and ethical business requirements, as such are provided below.

You, the undersigned, represent and warrant that you comply, and will continue to comply, for the duration of the services provided by you under the definitive agreement signed between you and Contentsquare (the "Agreement"), with the following requirements:

1. **Comply with all Applicable Laws in connection with the performance of your services under the Agreement.** "Applicable Laws" shall mean any applicable international, country, federal, state, and local law, ordinances, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance, industry code of practice, rule of court or directives, binding court decision or precedent, or delegated or subordinate legislation, licenses, permits and approvals as required by any government or authority for the performance the services under the Agreement, each of the above as may be amended from time to time;

2. **Comply with Contentsquare's Supplier Business Standards, as such are attached as Exhibit A to this document;**

3. In case you have access and/or interface with Contentsquare Data and/or Systems (either directly or indirectly), **comply with Contentsquare's Security Requirements, as such are attached as Exhibit B to this document.** "System" shall mean any computer system, application, or network owned, leased, licensed or otherwise used by Contentsquare. "Contentsquare Data" shall mean any information received from or about Contentsquare or its customers, either directly or indirectly, in any form (including, without limitation, technical information, customer information, personal information and/or employee information); and

4. In case you store, use, have access to or control over Contentsquare Data (either directly or indirectly) that includes personal information (as such is defined under Applicable Law), **comply with the terms of such Data Processing Agreement as shall be signed by you and Contentsquare and be deemed part of this document and the Agreement; and**

In any case in which it is determined by Contentsquare that you are in breach of this document, then Contentsquare may: (i) immediately suspend any further performance by you under the Agreement; and/or (iii) terminate the Agreement without penalty.

Signed for and on behalf of _____

Signature _____
Name _____
Designation _____
Date _____

v1.2020

- Exhibit A –

Contentsquare Supplier Business Standards

Contentsquare is committed to ethical business practices, and we hold our suppliers to the same high standards. These standards reflect our internal values and the expectations of our suppliers. We find that business relationships are more productive and effective when they are built on trust, mutual respect and common values, and seek relationships with suppliers who share a common commitment to such values.

Compliance with Law, Rules and Regulations

Our suppliers must comply with all applicable laws, rules, regulations, and ethical standards of the country in which they operate, as well as these standards.

Anti-Corruption

Our suppliers are prohibited from offering or receiving anything of value to obtain or retain business, an improper advantage, or favored treatment from any third party (including Government Officials), or any other person with whom Contentsquare or such supplier does or anticipates doing business. Our suppliers are required to keep accurate and transparent records that reflect actual transactions and payments. Our suppliers shall not participate in any corrupt, unethical or illegal practices.

Anti-Money Laundering

Our suppliers must conduct integrity assessments and other due diligence and be familiar with their business practices, observe and record payments and transactions consistent with all established policies and procedures. Our suppliers must immediately alert Contentsquare of any suspicious activity and cooperate fully with legal and regularity authorities charged with enforcing anti-money laundering laws.

Conflict of Interest

Contentsquare employees and personnel are required to avoid not only conflicts of interest but activities that could give the appearance that a supplier has improperly influenced such personnel in order to receive favorable treatment.
Our suppliers are required to avoid actions that may result in conflicts of interest, which include offering, providing or reimbursing personal gifts, favors, personal travel expenses, lodging or other housing, services of any kind, excessive meals or entertainment, or any other thing of value to Contentsquare employees and personnel.

Confidentiality Security and Insider Trading

All information about Contentsquare and our operations, products and personnel obtained as a consequence of relationship with Contentsquare which you have reason to believe is not publicly known, or which Contentsquare seeks to protect as confidential or proprietary, or which might be of use to competitors or harmful to Contentsquare or its customers, should be treated confidentially and not be disclosed. We expect our suppliers to comply with applicable security and privacy laws, regulations and retention requirements, and to ensure that they have appropriate technical and security controls in place to protect our information. Any non-public information obtained as a consequence of relationship with Contentsquare Shall not be used for the personal benefit of the supplier, its employees or any other person.

Intellectual Property

We expect our suppliers to respect our (and any other person's) intellectual property rights. Intellectual property rights are to be respected and transfer of technology and know-how is to be done in a manner that protects intellectual property rights.

Privacy

Our suppliers must respect the privacy of employees, customers and others whose personal information they have access to, by complying with local and applicable international laws when collecting and storing personal information. When collecting personal information, suppliers must collect personal information only for legitimate business purposes, share only with those who are allowed access, protect in accordance with security policies, retain only for as long as necessary, and contractually obligate third parties with access to personal information to protect it.

Trade Controls

Our suppliers must comply with the all applicable import and export controls, sanctions, and other trade compliance laws of the United States and the laws of the applicable country(ies) where the transaction(s) occur(s).

Honesty and Fair Competition

Our suppliers must uphold standards for fair business practices including accurate and truthful advertising and fair competition. Our suppliers must not take advantage of anyone through manipulation, concealment, abuse of privileged information or misrepresentation of material facts.

Environment, Health and Safety

Our suppliers must provide a safe and healthy working environment that complies with local laws and minimizes occupational hazards. We seek suppliers that operate in compliance with all applicable environmental laws and work to minimize their use of natural resources and any negative impact their operations have on the environment.

Human Capital and Workplace Responsibilities

Our supplier must: (i) treat all employees and other personnel with dignity and respect; (ii) comply with all applicable employment laws and regulations including statutes prohibiting discrimination in the workplace; (iii) not engage in any form of slavery, human trafficking, procure commercial sex acts or use forced labor; (iv) maintain a workplace free from harassment and discrimination; (v) not treat or threaten to treat an individual harshly or inhumanely; (vi) not employ or use underage labor in the production of their goods or services; and (vii) maintain a code of ethics that it shall require its employees and other personnel to understand and follow.

Whistleblowing

Our suppliers must allow and encourage their personnel to freely bring any information relating to the improper accounting or auditing practices, illegal or unethical conduct or conflicts of interest in connection with the finances or other aspects of operations of the company, to the proper appointed point of contact. Such appointed person must follow a strict and established procedure to investigate such allegations promptly in a manner appropriate to the circumstances, and report to the company's highest authority. The confidentiality of the identity of any person providing information regarding actual or alleged illegal conduct will be maintained to the extent possible, without impeding the investigation and resolution of the mater. Our suppliers commit that no employee will punish or retaliate against anyone who refuses to participate in misconduct, anyone who cooperates with an investigating agency, or anyone who engages in good faith reporting of information.

Equal Opportunity and No Discrimination

At Contentsquare we believe everyone deserves an equal chance to succeed and contribute. Our suppliers must never discriminate or deny equal opportunity. They must ensure that they contribute to providing equal opportunity to all employees and applicants and that they provide a work environment that is free from any type or form of discrimination. All decisions must be based on merit, qualifications and performance and never on characteristics such as gender, race, color, ethnicity, disability, religion, age, sexual orientation, or any other characteristics that are protected by law. Any discrimination must be reported immediately to the appropriate designated authority.

Monitoring and Compliance

Contentsquare may engage in monitoring activities to confirm suppliers' compliance to these standards, including on-site assessments of facilities, use of questionnaires, review of available information or other measures necessary to review such supplier performance. Contentsquare may disqualify any potential supplier or terminate any relationship with a current supplier that has failed to conform to these standards.

- Exhibit B –

Contentsquare Security Requirements

Contentsquare requires that all Suppliers that access and/or interface with any Systems and/or Scoped Data, either directly or indirectly, comply with all Applicable Laws and with all the requirements as set forth under these Contentsquare Security Requirements, if and as applicable to the services and/or products provided by Supplier to Contentsquare under such applicable Agreement (together, the "Security Requirements"), at their own expense. These Security Requirements establish a minimum set of controls that must be followed in order to protect Contentsquare Systems and Scoped Data. In the event of a conflict between the Agreement and these Security Requirements, the conflict will be interpreted to provide the greatest security protections to Contentsquare's Systems and Scoped Data .

Supplier must implement the below Security Requirements in its systems, processes and policies, and ensure the applicability of these Security Requirements upon any of its third party providers.

All capitalized terms not defined in the Definitions provision below, shall have the meanings set forth in the Statement of Compliance or the Agreement.

1. Certification

a. Supplier will, on an annual basis, obtain a formal review of its security controls conducted by an unaffiliated third party, and will thereafter provide Contentsquare with the written results of the audit and proof of Supplier's compliance with the audit requirements and/or Supplier's remediation plan. The specific third party audit type may be set forth in the Agreement. If not specified in the Agreement, Supplier will obtain a one of the audits provided as relevant examples below, which will be consistent with the services and/or products provided by the Supplier.

b. Prior to Processing Scoped Data, and upon any request by Contentsquare thereafter, Supplier will provide ContentSquare with copies of such certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Scoped Data. Supplier will promptly notify ContentSquare if Supplier has failed or no longer intends to adhere to such certifications or successor frameworks.

c. Examples of potentially relevant certifications include: SSAE 16 – SOC2; ISO 27001:2013; ISO 27018:2014; Payment Card Industry Data Security Standards (PCI-DSS); and Federal Information Security Management Act (FISMA) Compliance Certification.

2. Organization of information security

a. Supplier shall appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s), with responsibility and accountability for information security within the organization.

b. Supplier shall ensure that all information security responsibilities are defined and allocated in accordance with Supplier's approved policies for information security. Such policies shall be published and communicated to employees and relevant external parties.

c. Supplier shall have a risk management framework and conduct a yearly risk assessment of its environment and Systems to understand its risks and apply appropriate controls to manage and mitigate risks before offering its services.

3. Human resources security

a. Supplier shall inform its personnel about relevant security procedures and their roles and ensure that personnel with access to any Systems and/or Scoped Data are subject to written confidentiality obligations.

b. Supplier shall further inform its personnel of possible consequences of breaching Supplier's security policies, procedures and these Security Requirements, which must include disciplinary action and the ability to termination the contract with such employee or third party provider upon such breach.

c. Supplier personnel with access to any Systems and/or Scoped Data shall receive annual training covering these Security Requirements, additional privacy and security procedures that may be applicable to the services provided, prevention of unauthorized use or disclosure of Scoped Data and response to any Information Security Incidents.

d. Supplier shall perform relevant and appropriate background checks on any of its personnel and third party providers with access to any Systems and/or Scoped Data, all in compliance with Applicable Laws and .

4. Asset Management

a. Assets associated with any Systems and/or Scoped Data, including Supplier's information processing facilities shall be identified, and an inventory of these assets shall be maintained. Such inventory shall be provided to Supplier upon request.

b. Supplier shall classify, categorize, and/or tag Scoped Data to help identify it and to allow for access to it to be appropriately restricted.

5. Access control

a. Supplier shall restrict access to Scoped Data and Systems at all times solely to those individual personnel and third party providers whose access is essential to the Performance under the Agreement.

b. Supplier shall immediately suspend or terminate the access rights to Scoped Data and Systems for any Supplier's personnel or third party providers suspected of breaching any of the provisions of these Security Requirements or any Applicable Laws; and Supplier shall remove access rights of all employees or any third party providers immediately upon suspension or termination of their employment, contract, or agreement.

c. Supplier shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Scoped Data and/or Systems. Supplier shall use an enterprise access control system

that requires its personnel and third party providers revalidation by managers at regular intervals based on the principle of “least privilege” and need-to-know criteria based on job role.

d. Supplier shall maintain and update a record of personnel and third party providers authorized to access the Systems or any Scoped Data and Supplier shall review users’ access rights at least every 6 months.

6. Authentication

a. Where authentication mechanisms are based on passwords, Supplier shall require the password to conform to very strong password control parameters. The following rules must be implemented regarding passwords complexity:
    i. Minimum of eight characters long
    ii. Include lower cases
    iii. Include upper cases
    iv. Include numbers
    v. Include special characters

b. Passwords must be updated on a regular basis to prevent the possibility to be guessed or broken, in particular:
    i. The new password must differ from the previous 5 passwords
    ii. The new password must not have been used within the past 2 months

c. As per the most recent NIST requirements, automatic password rotation will not be forced anymore and compensatory controls have been implemented instead.

d. Password breaches must be monitored.

e. Users must be able to change their own password at any time (e.g., there is to be no minimum validity period) and administrators must be able to force a password change. In particular, this must be performed in case of breach or suspected leakage.

f. To limit the possibility of leakage, it must be ensured that passwords never appear in plain text when entered. Moreover, to prevent a malicious individual from guessing the password by errors and trials, access is to be suspended after 5 incorrect attempts.

g. Supplier shall use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage (e.g., passwords shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential passwords.

h. Use of multi-factor authentication if supported

7. Cryptography

a. Supplier shall have a policy on the use of cryptographic controls based on assessed risks.

b. Supplier shall assess and manage the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths. The following minimum level must be followed:

i. Symmetric algorithm to be used is AES with key length of at least 256 bits
ii. Asymmetric algorithms to be used is RSA (2048 bits at least) or elliptic curves (same level)
iii. Hash functions to be used are at least SHA256. A salt must be used in addition for password hashing.
iv. TLSv1.1 or TLSv1.2 for in transit encryption (SSLv2 and SSLv3 must be rejected)

c. Supplier's cryptographic controls/policy shall address appropriate algorithm selections, key management and other core features of cryptographic implementations.

d. Supplier shall have procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.

8. Physical and Environmental Security

a. Supplier shall limit access to facilities where systems that process Scoped Data are located to authorize individuals and use a variety of industry standard systems to protect against loss of data due to power supply failure, line interference or others environmental related failures:

i. 7*24security guard, alarms and CCTV
ii. Log of all physical access with 90 days minimum log retention, access review every 6 months
iii. Fire protection: Air sampling and automatic fire extinguisher deigned to not damage electronic, 1 year maintenance frequency
iv. Temperature protection: Redundant air conditioner with the appropriate temperature (18– 27 °C), 1 year maintenance frequency
v. Water protection: Water leak protection
vi. Humidity protection
vii. Power failure protection: Redundant UPS and redundant power generator, 1 year maintenance frequency

9. Operations security

a. Supplier shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to any Systems and/or Scoped Data and to its systems and networks. Supplier shall ensure the policies are communicated to all its personnel and third party providers involved in the processing or have access to any System or Scoped Data.

b. The standards and procedures shall meet or exceed industry best practices and applicable regulations and laws, and include, without limitation: security controls; identification and patching of security vulnerabilities; change control process and procedures; problem management; and incident detection and management.

c. Supplier shall maintain logs of administrator and operator activity and data recovery events

d. Supplier shall have a documented security program and policies that provide guidance to its personnel and third party providers to ensure the security, confidentiality, integrity, and availability of the Scoped Data and Systems maintained or processed by Supplier, and that provides express instructions regarding the steps to take in the event of a compromise or any Information Security Incident.

10. Communication security and data transfer

a. Supplier shall, at a minimum, use the following controls to secure its networks which store Scoped Data:
   i. Network traffic shall pass through firewalls, which are monitored at all times. Supplier must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.
   ii. Access to network devices for administration must utilize a minimum of 256-bit, industry standard encryption.
   iii. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters, upper case, lower case, numeral, special character) and be changed at least every 180 days.
   iv. Initial user passwords are required to be changed during the first log-on. Supplier shall have a policy prohibiting the sharing of user IDs and passwords.
   v. Firewalls must be deployed to protect the perimeter Scoped data.

b. When remote connectivity is required for processing of Scoped Data, Supplier shall use VPN servers for the remote access with the following or similar capabilities:

   i. Connections must be encrypted using a minimum of 256-bits encryption.
   ii. The use of multi -factor authentication is required.

c. Supplier shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to these Security Requirements. Such policies shall be designed to protect transferred information from interception, copying, modification, corruption, mis-routing and destruction.

11. System Acquisition, Development, and Maintenance

a. Supplier shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. Supplier shall have policies for secure development, system engineering, and support. Supplier shall conduct appropriate tests for system security as part of acceptance testing processes Supplier shall supervise and monitor the activity of outsourced system development.

c. Supplier will perform annual penetration test on their internet perimeter network.

d. Supplier shall respond promptly to all reasonable security audit, scanning, discovery, and testing reports requested from Contentsquare, or from regulators (to the extent required by law) and shall cooperate and assist those regulators as required by law.

e. If any audit or penetration testing exercise referred to above reveals any deficiencies, weaknesses or areas of non-compliance, Supplier shall promptly take such steps as may be required to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable in the circumstances.

f. Supplier shall keep Contentsquare informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Contentsquare as soon as may be practicable in the circumstances that all remedial actions have been completed.

12. Management of Information Security Incidents and Improvements

a. Supplier shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

b. Supplier shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as possible. All Supplier employees and third party providers should be made aware of their responsibility to report Information Security Incidents as quickly as possible.

c. Supplier shall maintain a record of Information Security Incidents with a description of the incident, the consequences of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to correct future security incidents.

13. Information Security Aspects of Business Continuity Management

a. Supplier shall maintain emergency and contingency plans for the facilities in which Supplier information systems that process Scoped Data are located. To ensure that they are valid and effective during adverse situations, Supplier shall verify the established and implemented information security continuity controls at regular intervals.

b. Supplier's redundant storage and its procedures for recovering data shall be designed to reconstruct Scoped Data in its original state from before the time it was lost or destroyed.

14. Notification and Communication Obligations

a. Supplier shall immediately (i.e., within 48 hours) notify ContentSquare's security team (security@contentsquare.com) if any of the following events occur:

i. any Information Security Incident or compromise of any System or Scoped Data;
ii. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of information that is processed, stored and transmitted using a computer in connection with Scoped Data;
iii. failure or inability to maintain compliance with these Security Requirements or Applicable Laws

15. Audit clause

a. Contentsquare may perform yearly audits, or at any other time in case of suspected Information Security Incident, to ensure that Supplier follow these Security Requirements, providing a 30 days notice, unless it is due to a suspected Information Security Incident.

16. Definitions

Information Security Incident	Means a suspected, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of Scoped Date or to Contentsquare Systems; interference with information technology operations; interference with system operations; or breach by Supplier of Applicable Laws which impacts the privacy or security of Scoped Data, Contentsquare Systems or Supplier systems.
Performance	Means any acts by the Supplier in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Scoped Data, or providing Software as a Service ("SaaS"), cloud platforms or hosted services.
Scoped Data	Means all Contentsquare Data and any information and data provided or made available to Supplier, including customer information and data, any manipulation of that data and any data or information Supplier collects, generates, or otherwise obtains in connection with its Performance under the Agreement.
Supplier	Means the person or legal entity, regardless of the form of organization that has entered into an Agreement with ContentSquare.